UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/698,159	10/30/2000	Anup K. Ghosh	CIG-103	7526

7590 04/07/2004

Brett C. Martin
1650 Tyson Blvd.
McLean, VA 22102

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	7

DATE MAILED: 04/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/698,159	GHOSH ET AL.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 October 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed 30 October 2000 with a continuing application priority date of 28 October 1999.

2. Claims 1-50 are currently pending in this application. Claims 1, 12, 23 and 37 are independent claims.

3. The use of the trademarks UNIX and WINDOWS NT has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Objections

4. Claims 3, 14, 25, and 39 contain the trademark/trade name UNIX. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe an operating system and, accordingly, the identification/description is indefinite.

5. Claims 4, 15, 26, and 40 contain the trademark/trade name WINDOWS NT Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe an operating system and, accordingly, the identification/description is indefinite.

6. **Claim 22** is objected to because of the following informalities: Claim 22 indicates: "A detection system of claim 12", it appears that applicant indicated "detection system" where "method" was intended because claim 12 is a method. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 9-11, 20-22, 31, 31, 45, and 46 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claims contain

subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The claims indicate a "detection system" or "method" "characterized by a false positive rate less than" a numeric percentage and "a false negative rate less than" a percentage. The specification does not indicate the method or the numeric percentage rates provided.

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 9-11, 20-22, 31, 31, 45, and 46 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear how the percentages provided relate to the previous claims.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Claims 9-11, 20-22, 31, 31, 45, and 46 are rejected under 35 U.S.C. 101 because the claimed invention is not supported by either a specific, substantial and credible asserted utility or a well established utility.

The claims are directed toward an intrusion detection system or method, which is characterized by false positive and false negative rates theses rates are dependent on numerous various factors which cannot be claimed in an invention. A false positive

could be due to various equipment failures i.e. hardware, software, network traffic, user error the amount of these errors cannot be controlled or anticipated because the errors are not in a closed constant environment. The network environment or Internet is constantly changing therefore intrusion detection false positives rates are impossible to predict.

Claims 9-11, 20-22, 31, 31, 45, and 46 are also rejected under 35 U.S.C. 112, first paragraph. Specifically, since the claimed invention is not supported by either a specific, substantial and credible asserted utility or a well established utility for the reasons set forth above, one skilled in the art clearly would not know how to use the claimed invention.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

14. **Claims 1, 2, 5, 7, 8, 12, 13, 16, 18, 19, 23, 24, 27, 29, 30, 37, 38, 41, 43, and 44** are rejected under 35 U.S.C. 102(e) as being anticipated by Munson et al. U.S. Patent No. 6,681,331 (hereinafter '331).

As to independent claim 12, "A method for detecting intrusive behavior" is taught in '331 col. 2, lines 10-11;

"in a first session on a computer, said first session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said method comprising the steps of:" is shown in '331 col. 6, lines 30-34;

"(a) creating a plurality of first application profiles, wherein each said first application profile comprises a plurality of first data strings, wherein each first data string comprises a sequential mapping of instructions passed from one of said plurality of applications to the computer operating system during a second session on the computer" is disclosed in '331 col. 7, lines 17-20;

"(b) creating a plurality of second application profiles, wherein each second application profile comprises a plurality of application segments, wherein each application segment comprises a pre-determined number of second data strings, wherein each second data string comprises a sequential mapping of instructions passed from one of said applications to the computer operating system during the first session on the computer" is taught in '331 col. 9, lines 49-55;

"(c) initializing an application counter;

(d) initializing a plurality of segment counters, wherein each segment counter corresponds to one of the second application profiles" is shown in '331 col. 8, lines 16-37;

"(e) initializing a plurality of data string counters, wherein each data string counter corresponds to one of the application segments in the plurality of application segments" is disclosed in '331 col. 13, lines 2-3 and col. 14, lines 25-26;

"(f) performing an equality matching algorithm, wherein for each application segment, each second data string is compared to the plurality of first data strings comprising a corresponding application profile, and wherein if the second data string is not equal to any of the first data strings an associated data string counter is incremented; and

(g) performing a temporal locality identifying, algorithm, wherein the first session is labeled intrusive if a ratio of the segment counter to a total number of segments in an associated second application profile exceeds an application threshold and wherein the first session is labeled intrusive if a ratio of the application counter to a total number of applications exceeds a session threshold, wherein the application counter is incremented if a ratio of an associated segment counter to a total number of segments in an associated second application profile exceeds a segment threshold, wherein the associated segment counter is incremented if a ratio of an associated data string counter to the pre-determined number of data strings comprising the segment exceeds an associated data string threshold" is taught in '331 col. 4, lines 26-65.

As to dependent claim 13, "wherein the second session comprises non-intrusive behavior" is shown in '331 col. 4, lines 30-33.

As to dependent claim 16, "herein the first plurality of application profiles and second plurality of application profiles are created by a data pre—processor application" is disclosed in '331 col. 4, lines 33-40.

As to dependent claim 18, "wherein the data pre-processor creates the second plurality of application profiles in real-time" is taught in '331 col. 6, lines 11-12

As to dependent claim 19, "wherein the equality matching algorithm and the temporal locality identifying algorithm receive input from the second plurality of application profiles in real-time" is shown in '331 col. 6, lines 11-15.

As to independent claim 1, this claims is directed to the detection system of the method of claim 12 and is similarly rejected along the same rationale.

As to dependent claims 2, 5, 7, and 8, these claims incorporate substantially similar subject matter as in cited in claims 13, 16, 18, and 19 above and are rejected along the same rationale.

As to independent claim 37, "A method for detecting intrusive behavior" is taught in '331 col. 2, lines 10-11;

"in a session on a computer, said session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said method comprising the steps of" is shown in '331 col. 6, lines 30-34;

"(a) training a plurality of neural networks, wherein each neural network is trained to identify a pre-determined behavior pattern for a corresponding one of the plurality of applications" is disclosed in '331 col. 7, lines 17-20;

"(b) creating a plurality of application profiles, wherein each application profile comprises a plurality of application data for a corresponding one of the plurality of applications, wherein said application data is collected during the session" is taught in '331 col. 9, lines 49-55;

"(c) performing a temporal locality identifying algorithm, wherein when one of the plurality of application profiles is sequentially input to a corresponding one of the plurality of neural networks the neural network outputs a behavior indicator for each of the plurality of data strings in the application profile, and wherein if the behavior indicator meets a pre-determined criteria, a counter is incremented, and wherein if the counter has a high rate of increase the temporal locality identifier labels the application behavior intrusive, and wherein if a predetermined percentage of application behaviors are intrusive the session behavior is labeled intrusive" is taught in '331 col. 4, lines 26-65.

As to dependent claims 38, 41, 43, and 44 these claims incorporate substantially similar subject matter as in cited in claims 13, 16, 18, and 19 above and are rejected along the same rationale.

As to independent claim 23, this claim is directed to the detection system of the method of claim 37 and is similarly rejected along the same rationale.

As to dependent claims 24, 27, 29, and 30 these claims incorporate substantially similar subject matter as in cited in claims 13, 16, 18, and 19 above and are rejected along the same rationale.

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. **Claims 3, 4, 6, 9-11, 14, 15, 17, 20-22, 25, 26, 28, 31, 32, 39, 40, 42, 45, and 46** are rejected under 35 U.S.C. 103(a) as being unpatentable over '331 in further view of Rowland U.S. Patent No. 6,405,318 (hereinafter '318).

As to dependent claim 17 the following is not taught in '331 **"wherein the data pre-processor receives input from an auditing system integral to the computer operating system"** however '318 teaches "The system combines the above listed capabilities with real-time monitoring of log audit files, port scan detection capability and session monitoring" in col. 2, lines 65-68.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the intrusion detection system taught in '331 to include a means to utilize audit reports to improve intrusion detection. One of ordinary skill in the art would have been motivated to perform such a modification to automatically build user profiles see '318 (col. 2, lines 40 et seq.) "The present invention provides a real-time intrusion

detection method and system. The intrusion detection system automatically and dynamically builds user profile data".

As to dependent claim 14 "wherein the computer operating system comprises a UNIX operating system and the sequential mapping of instructions comprise a sequential mapping of UNIX system calls" is taught in '318 col. 4, lines 34-40 "for a Unix® based operating system or may be event logs for a Windows NT® operating system. The system checks to determine if the user should be ignored".

As to dependent claim 15 "wherein the computer operating system comprises a Windows NT operating system, and wherein the sequential mapping, of instructions comprises a sequential mapping of object requests" is shown in '318 col. 4, lines 34-40 "for a Unix® based operating system or may be event logs for a Windows NT® operating system. The system checks to determine if the user should be ignored".

As to dependent claims 20-22, "characterized by a false positive rate less than ... and a false negative rate less than ..." is shown in '318 col. 8, lines 37-40 "The system administrator may also alter the alarm thresholds or use preprogrammed alarm thresholds".

As to dependent claims 3, 4, 6, and 9-11 these claims incorporate substantially similar subject matter as in cited in claims 14, 15,17, and 20-22 above and are rejected along the same rationale.

As to dependent claims 25, 26, 28, 31, and 32 these claims incorporate substantially similar subject matter as in cited in claims 14, 15,17, and 20-22 above and are rejected along the same rationale.

As to dependent claims 39, 40, 42, 45, and 46 these claims incorporate substantially similar subject matter as in cited in claims 14, 15,17, and 20-22 above and are rejected along the same rationale.

17. **Claims 33-36 and 47-50** are rejected under 35 U.S.C. 103(a) as being unpatentable over '331 in further view of Bergman et al. U.S. Patent No. 6,442,694 (hereinafter '694).

As to dependent claim 47, the following is not taught in '331 **"wherein the plurality neural network comprises a plurality of backpropogation neural networks"** however '694 teaches "In describing the processing which take place at a particular nodes, it is useful to define some terms related to the timing of such processing. Time delays for processing an d transmission of messages at each of nodes 42 are denoted as follows:" in col. 11, lines 50-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the intrusion detection system taught in '331 to include a means to examine the backpropogation of the network. One of ordinary skill in the art would have been motivated to perform such a modification to improve intrusion detection system see '694 (col. 5, lines 9 et seq.) "In view of the above, it has been recognized that since the results of component failures and attacks are often similar (e.g. improper operation of one or more network components or nodes), the difference is transparent ot a

network nor or system user. Because of this transparency there is no absolute metric to determined whether an input is fault or not".

As to dependent claim 48, "herein each neural network in the plurality of backpropogation neural networks comprises an input layer, a hidden layer and an output layer" is taught in '694 col. 15, lines 19-26 "From the above processing steps it can be seen that no node will generate an alarm until at least one attack is detected. When an attack occurs only the first node experiencing the attack will respond with an alarm. All nodes downstream from the first node receive messages which indicate that the node upstream experienced an attack".

As to dependent claim 49, "wherein a number of nodes in the hidden layer is determined by testing a plurality of cases for each neural network in the plurality of backpropogation neural networks and selecting the case wherein the corresponding neural network has a highest accuracy rate" is shown in '694 col. 6, lines 35-48 "The test on a unit to determine whether it is faulty or operational is reliable only for operational units. Necessary and sufficient conditions for the testing structure for establishing each unit as faulty or operational as long as the total number of faulty elements is under some bound are known".

As to dependent claim 50, "wherein the plurality of neural networks comprises a plurality of recurrent neural networks" is disclosed in '694 col. 10, lines 9-21 "It should be noted that the techniques of the present invention have applicability to a wide variety of different types of networks and is advantageously used in theses application".

As to dependent claims 33-36 these claims incorporate substantially similar subject matter as in cited in claims 47-50 above and are rejected along the same rationale.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

McNabb et al. U.S. Patent No. 6,289,462 issued dated: Sep. 11, 2001

Drake et al. U.S. Patent No. 6,347,374 issued dated: Feb. 12, 2002

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Ellen Tran
Patent Examiner
Technology Center 2134
30 March 2004